

REMARKS*Claim Amendments*

Applicants respectfully request entry of the foregoing claim amendments, which amend Claims 1 and 20. Support for the claim amendments can be found at Page 4, lines 5-6, and Page 12, lines 11-13, among other places. No new matter is introduced.

Rejections under 35 U.S.C. §103

Claims 1-2, 7-8, 16-21, 25-30, 34-37 and 40-41 are rejected under 35 U.S.C. §103 due to U.S. Pat. No. 6,081,793 of Challener *et al.* (here, “Challener *et al.*”) in view of U.S. Pat. No. 5,903,652 of Mital (here, “Mital”), and further in view of the article “How to Share a Secret” by Adi Shamir, from the *Communications of the ACM*, November 1979, Vol. 22, No. 11 (here, “Shamir”), and further in view of Schneier (“Applied Cryptography,” Second Edition, 1996).

Dependent Claims 4, 9-12, 23 and 27-30 are rejected under 35 U.S.C. §103 due to Challener *et al.* in view of Mital, and further in view of Shamir and Schneier. It is noted that remarks in the Office Action refer to a “Stallings” reference as having been cited against Claims 1 and 20; however, no Stallings reference was cited against Claims 1 and 20. Applicants therefore assume that the reference to Stallings is a typographical error, and that the rejection of these dependent Claims is intended to be based on Challener *et al.*, Mital, Shamir and Schneier.

Dependent Claims 13-15, 31-33 and 38 are rejected under 35 U.S.C. §103 due to the same references as in the previous grouping of dependent claims, and further in view of U.S. Patent No. 6,151,631 of Ansell *et al.* (here, “Ansell *et al.*”). Again, the reference to “Stallings” in remarks in the Office Action is assumed to be a typographical error.

Dependent Claim 39 is rejected under 35 U.S.C. §103 due to Challener *et al.* in view of Mital and Shamir and Schneier, and further in view of European Patent EP 0 909 074 A1 of Coss *et al.*

Independent Claims 1 and 20

To address the concern stated in the most recent Office Action that the claims do not include the concept of a reversible mapping, Applicants have amended independent Claims 1 and

20 to recite that the communications module is “capable of... transmitting from the receiver to the sender a return of the working data based on a reverse mapping performed by the mapping module.”

With these amendments, Applicants respectfully submit that Challener *et al.* in view of Mital, and further in view of Shamir and further in view of Schneier does not disclose or suggest the claimed mapping module in combination with the other features of independent Claims 1 and 20, as amended.

As discussed in the previous Amendment, Applicants’ Claims 1 and 20 involve, among other things, a mapping module that anonymously maps the personal identifier portions of working data so that a receiver obtains anonymous data, while leaving the research data portion unmapped by the anonymous mapping. The identifier portions and the research data portions of the working data are transmitted over a secure communications channel, which is formed by a sender being authenticated with a communication module and a receiver being authenticated with the communication module. Keyholder access to the mapping module is controlled by a secret sharing module. Such a system may be used, for example, to allow a scientist to study research data collected from patients without being able to access the patients’ personal identities.

Because the present amendments recite that the working data may be returned based on a reverse mapping performed by the mapping module, it is made clear that a further advantage of Claims 1 and 20 is, for example, to allow the scientist to return the anonymous data packets to the original sender, by a reverse mapping. The original sender may therefore obtain data that can be identified by personal identifiers. The scientist could mark records of patients found to be in an at-risk group for a disease or condition, without knowing the personal identifiers for the individuals in that group, and return all of the records to the original sender with those records marked. The original sender could then contact those individuals to provide medical advice to the at-risk group.

The cited combination of Challener *et al.* in view of Mital, and further in view of Shamir and further in view of Schneier does not disclose or suggest such an apparatus having all of the claimed components, or the corresponding method of independent Claim 20.

Challener *et al.* does not disclose or suggest an apparatus or method having the anonymous, reversible mapping of amended Claims 1 and 20, because Challener *et al.* does not allow the results server to return a vote to the voter along with an indication of the voter's identity. Instead, the results server of Challener *et al.* receives the vote only with an "add" message, and is unable to return a message to the voter with the voter's identity. Challener *et al.* therefore does not disclose or suggest an anonymous reversible mapping, as in amended Claims 1 and 20, along with the other elements of those claims.

Mital likewise does not disclose or suggest such an anonymous reversible mapping, along with the other elements of amended Claims 1 and 20, because Mital makes the consumer's personal identity available to the merchant, so that an order may be associated with the correct shipping information. The mapping of Mital between the consumer and the merchant is therefore not anonymous.

Shamir is directed to a technique for secret-sharing, and does not disclose or suggest a reversible mapping transmitting anonymous working data over a secure channel between a sender and receiver who are both authenticated with a communication module.

Likewise, Schneier does not disclose or suggest the anonymous, reversible mapping module and other components of Claims 1 and 20. The cited DASS protocol allows mutual authentication, but Schneier does not disclose or suggest using a reversible mapping to transmit working data anonymously over a secure channel created by authenticated both a sender and a receiver with a communications module.

Further, none of the cited combination of references discloses or suggests using secret sharing to control keyholder access to a system having both a communication module that creates a secure channel, and an anonymous, reversible mapping of working data between parties over that secure channel.

Therefore, because Challener *et al.* in view of Mital, and further in view of Shamir and further in view of Schneier does not disclose or suggest the inventions of independent Claims 1 and 20, Applicants respectfully request reconsideration and allowance of those claims.

Dependent Claims

In addition, because dependent Claims 2, 4, 7-19, 21, 23, and 25-41 incorporate the features of base Claims 1 and 20, they are also allowable for the foregoing reasons. Further, neither Ansell *et al.* nor Coss *et al.*, which are applied only to the dependent claims, discloses or suggests the claimed anonymous, reversible mapping in combination with the other features of independent Claims 1 and 20.

Applicants therefore submit that all of the dependent Claims are also allowable for the foregoing reasons.

CONCLUSION

In view of the above amendments and remarks, it is believed that all claims are in condition for allowance, and it is respectfully requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By 

Keith J. Wood

Registration No. 45,235

Telephone: (978) 341-0036

Facsimile: (978) 341-0136

Concord, MA 01742-9133

Date: 9/27/07